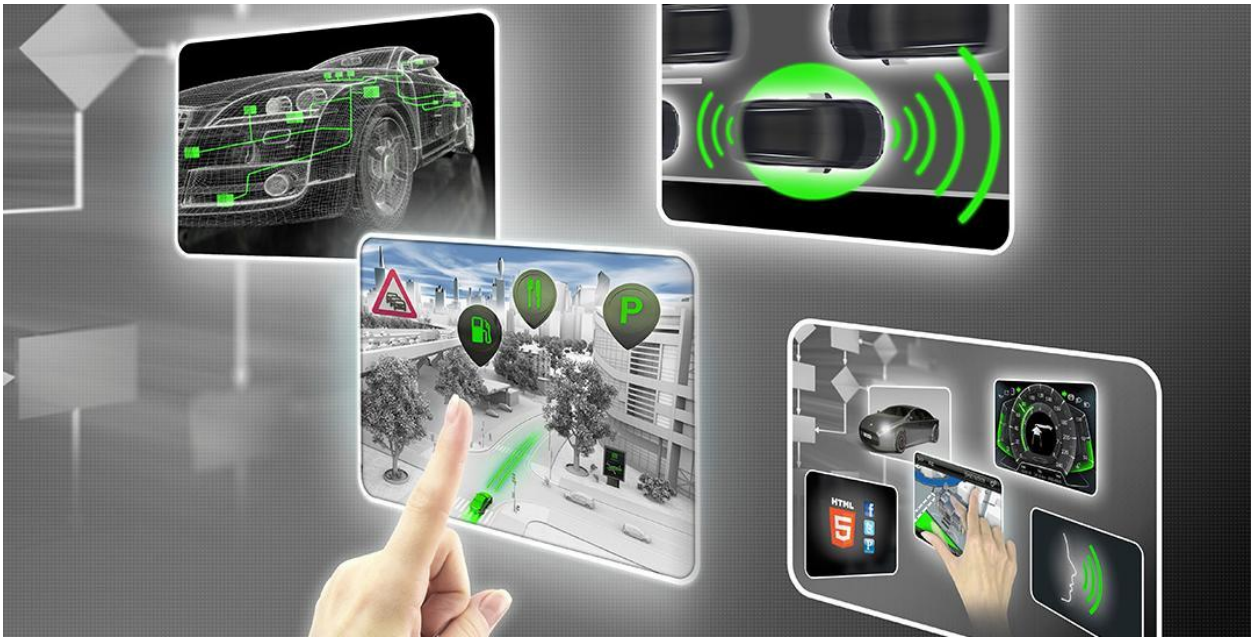
Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: 0.1



Document history

Date	Version	Editor	Description
30/05/2019	0.1	M. Elbanhawi	First draft

Table of Contents

Introduction

Purpose of the Safety Plan

A safety plan provides an overall framework for a functional safety of a Lane assistance item in a vehicle.

Scope of the Project

For the lane assistance project, the following safety lifecycle phases are in scope:

Concept phase
Product Development at the System Level
Product Development at the Software Level

The following phases are out of scope:

Product Development at the Hardware Level
Production and Operation

Deliverables of the Project

The deliverables of the project are:

Safety Plan
Hazard Analysis and Risk Assessment
Functional Safety Concept
Technical Safety Concept
Software Safety Requirements and Architecture

Item Definition

The item under consideration is a lane assistance system which is a subsystem of the Advanced Drivers Assistance System (ADAS) of a vehicle. The main functions of Lane Assistance, in the case of lane departure is to:

- Alert the driver in
- Take over control to keep the vehicle in the lane

The two functions in charge of alerting the driver and taking over control are referred to as:

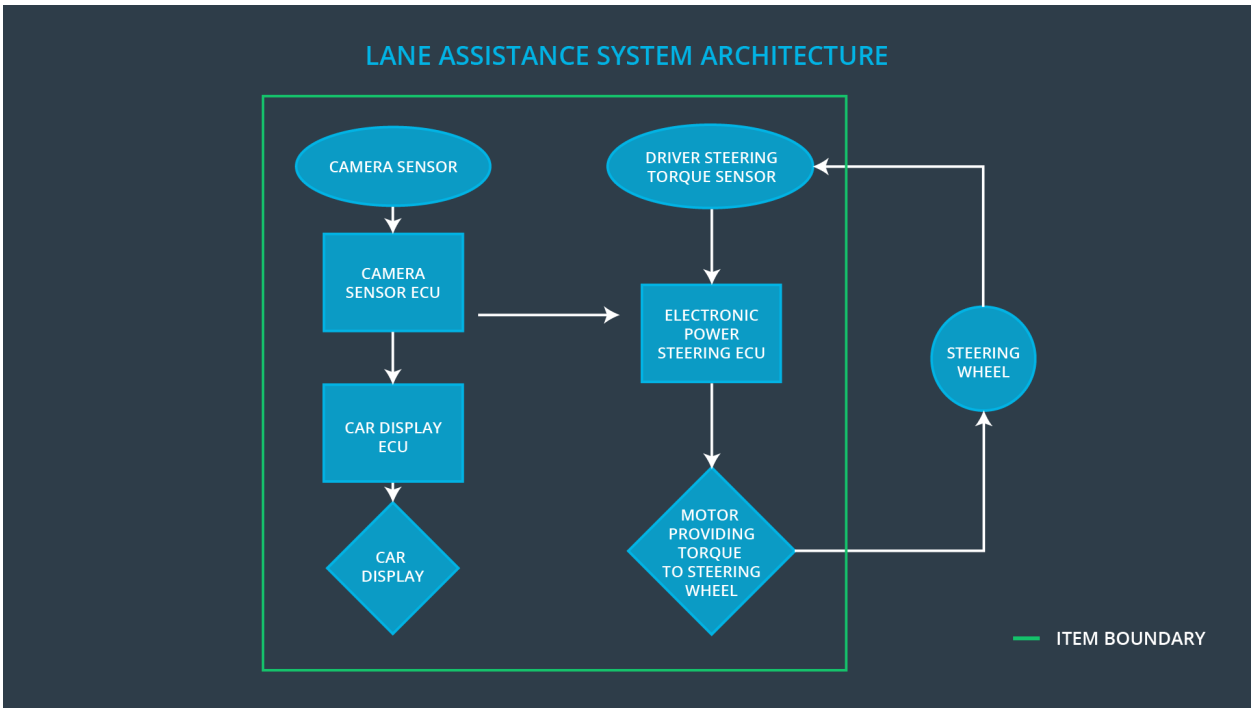
- Lane Departure Warning (LDW)
- Lane Keeping Assistance (LKA)

LDW is responsible for alerting the driving in the case of lane departure using the human machine interface (HMI) of the vehicle on the dashboard and vibrate the steering wheel by applying a torque to the steering wheel.

LKD is responsible for keeping the vehicle within the current lane in the case of lane departure. The system will apply a torque to the steering wheel to manoeuvre the vehicle back into the current lane.

There are three subsystems

- Electronic Power steering subsystem: Responsible for vibrating steering wheel and manoeuvring vehicle to the centre of the lane.
- Camera subsystem: Responsible for monitoring vehicle position in the lane and detecting lane departure.
- Car display subsystem: Responsible for alerting the vehicle.



Electronic Power Steering Subsystem elements:

- Electronic Power Steering torque sensor
- Electronic Power Steering ECU

Camera Subsystem elements:

- Camera sensors
- Camera sensor ECU

Car Display Subsystem elements:

- Car Display ECU
- Car Display

Goals and Measures

Goals

The goal of analysing the lane assistance functions with ISO 26262 is to identify the risks and hazards of the lane assistance functions. The risks are then evaluated. Finally, risks are lowers or mitigated.

Measures

Measures and Activities	Responsibility	Timeline
Follow safety processes	All team members	Constantly
Create and sustain a safety culture	All team members	Constantly
Coordinate and document the planned safety activities	Safety manager	Constantly
Allocate resources with adequate functional safety competency	Project manager	Within 2 weeks of start of project
Tailor the safety lifecycle	Safety manager	Within 4 weeks of start of project
Plan the safety activities of the safety lifecycle	Safety manager	Within 4 weeks of start of project
Perform regular functional safety audits	Safety auditor	Once every 2 months
Perform functional safety pre-assessment prior to audit by external functional safety assessor	Safety manager	3 months prior to main assessment
Perform functional safety assessment	Safety assessor	Conclusion of functional safety activities

Safety Culture

Here are some characteristics of a good safety culture:

- **High priority**: safety has the highest priority among competing constraints like cost and productivity
- **Accountability**: processes ensure accountability such that design decisions are traceable back to the people and teams who made the decisions
- **Rewards**: the organization motivates and supports the achievement of functional safety
- **Penalties**: the organization penalizes shortcuts that jeopardize safety or quality
- **Independence**: teams who design and develop a product should be independent from the teams who audit the work
- **Well defined processes**: company design and management processes should be clearly defined
- **Resources**: projects have necessary resources including people with appropriate skills
- **Diversity**: intellectual diversity is sought after, valued and integrated into processes
- **Communication**: communication channels encourage disclosure of problems

Safety Lifecycle Tailoring

For the lane assistance project, the following safety lifecycle phases are in scope:

Concept phase
Product Development at the System Level
Product Development at the Software Level

The following phases are out of scope:

Product Development at the Hardware Level
Production and Operation

Roles

Role	Org
Functional Safety Manager- Item Level	OEM
Functional Safety Engineer- Item Level	OEM
Project Manager - Item Level	OEM
Functional Safety Manager- Component Level	Tier-1
Functional Safety Engineer- Component Level	Tier-1
Functional Safety Auditor	OEM or external
Functional Safety Assessor	OEM or external

Development Interface Agreement

A DIA (development interface agreement) defines the roles and responsibilities between companies involved in developing a product. All involved parties need to agree on the contents of the DIA before the project begins.

The DIA also specifies what evidence and work products each party will provide to prove that work was done according to the agreement.

The ultimate goal is to ensure that all parties are developing safe vehicles in compliance with ISO 26262.

Role	Org	Tasks
Functional Safety Manager- Item Level	OEM	Pre- Plans, audits development phase
Functional Safety Engineer- Item Level	OEM	Develops prototypes, integrates subsystem into larger system
Project Manager - Item Level	OEM	Allocates resources as needed
Functional Safety Manager- Component Level	Tier-1	Pre- Plans, audits development phase for lane assistance item
Functional Safety Engineer- Component Level	Tier-1	Modifies OEM lane assistance subsystem, integrates lane assistance subsystem

Functional Safety Auditor	OEM or external	Ensures the project conforms to the safety plan
Functional Safety Assessor	OEM or external	Judgers whether the project has improved safety

Confirmation Measures

Confirmation measures serve two purposes:

- that a functional safety project conforms to ISO 26262, and
- that the project really does make the vehicle safer.

The people who carry out confirmation measures need to be independent from the people who actually developed the project.

Confirmation review:
Ensures that the project complies with ISO 26262. As the product is designed and developed, an independent person would review the work to make sure ISO 26262 is being followed.

Functional safety audit:
Checking to make sure that the actual implementation of the project conforms to the safety plan is called a functional safety audit.

Functional safety assessment:
Confirming that plans, designs and developed products actually achieve functional safety is called a functional safety assessment.

A safety plan could have other sections that we are not including here. For example, a safety plan would probably contain a complete project schedule.

There might also be a "Supporting Process Management" section that would cover "Part 8: Supporting Processes" of the ISO 26262 functional safety standard. This would include descriptions of how the company handles requirements management, change management, configuration management, documentation management, and software tool usage and confidence.

Similarly, a confirmation measures section would go into more detail about how each confirmation will be carried out.